BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

金融機関におけるモバイルアプリの提供状況と管理体制について
―アンケート調査結果から―

日本銀行
金融機構局
2022年11月

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

金融システムレポート別冊シリーズについて

日本銀行は、マクロ・プルーデンスの視点からわが国金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を行うことにより、『金融システムレポート』を補完するものである。本別冊では、2022 年 4 月から 5 月にかけて実施した「モバイルアプリの提供状況等に関するアンケート」の結果を紹介する。

本別冊の要旨

金融機関では、1990 年代後半以降、顧客利便性の向上や業務の効率化を企図して、インターネットを通じた金融取引サービスの提供・拡充を進めてきた。こうしたなか、近年では、スマートフォンをはじめとしたモバイル端末の保有率上昇等を背景に、対顧客接点として、モバイルアプリの新規開発や機能拡充に注力する動きがみられている。

日本銀行では、こうした金融機関の動向や、新型コロナウイルス感染症の拡大を受け、非対面型のサービスに対する人々のニーズが高まっている状況を踏まえて、取引先金融機関のうち 156 先を対象に、モバイルアプリの提供状況等を調査するため、アンケート調査を実施した。アンケート結果をみると、多くの金融機関がモバイルアプリを提供しているほか、モバイルアプリなどのデジタルチャネルは、今後も更なる利用増加を見込んでおり、対顧客チャネルのデジタル化、非対面化が今後も一段と進展していくとみられることが確認できた。

金融機関の対顧客チャネルにおけるデジタル化の進展は、顧客の利便性向上に資する一方、インシデントが発生した場合の顧客への影響度は大きくなる。平時から適切な開発・管理体制の下でモバイルアプリの脆弱性対応やセキュリティ対策を実施していくとともに、インシデント発生時を想定し、顧客に対してサービス停止の状況や代替サービス（店舗窓口、ATM 等）の案内といった情報が円滑に伝達されるよう業務継続体制を構築しておくことが重要である。チャネルごとの事務量の動向といった環境変化を踏まえた訓練（机上を含む）を定期的に実施することを通じて、想定している業務継続体制の実効性を検証するとともに、管理体制の更なる強化に繋げていくことが期待される。

日本銀行としても、今後も考査・モニタリングやセミナーなどを通じて、金融機関のこうした取り組みを後押ししていく方針である。

１．はじめに

金融機関では、1990 年代後半以降、顧客利便性の向上や業務の効率化を企図して、インターネットを通じた金融取引サービスである「インターネットバンキング」[1]の提供を始め、その後もサービスの拡充を進めてきた。こうしたなか、近年では、スマートフォンをはじめとしたモバイル端末の保有率上昇等を背景に、対顧客接点として、「モバイルアプリ」[2]の新規開発や機能拡充に注力する動きがみられている。

日本銀行では、こうした金融機関の動向のほか、新型コロナウイルス感染症の拡大を受けて、非対面型のサービスに対する人々のニーズが高まっている状況を踏まえて、取引先金融機関のうち 156 先[3]（以下、「調査先」という）を対象に、モバイルアプリの提供状況等を調査するためのアンケートを実施した[4]。

---

[1] 「インターネットバンキング」とは、インターネットを利用して金融機関が金融取引のサービスを提供することをいう。パソコンのほか、携帯電話やスマートフォンなどからも利用できるケースが多い。本稿では、ブラウザを経由して提供されるものをいう。

[2] 「モバイルアプリ」とは、本稿では、スマートフォンやタブレット端末等のモバイル端末向けに開発されたアプリケーションソフトウェアのうち、モバイル端末向けのアプリ配信プラットフォームに掲載され、モバイル端末等にダウンロードして利用されるものをいう。

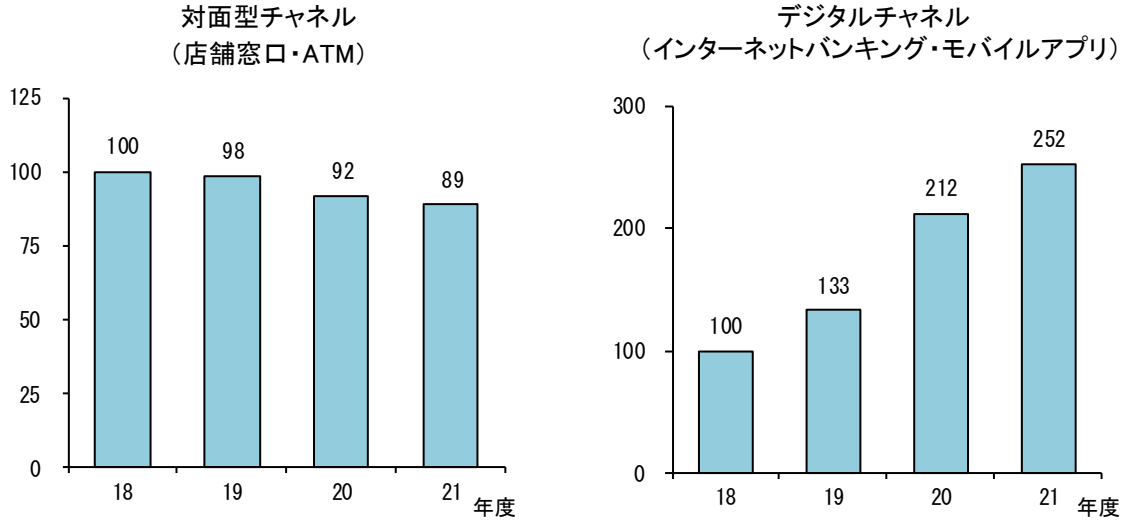
[3] 調査先の業態別内訳は、「大手行等」：みずほ、三菱 UFJ、三井住友、りそな、埼玉りそな、新生、あおぞら、ゆうちょ（8 行）。「ネット銀行等」：PayPay、セブン、ソニー、楽天、住信 SBI ネット、au じぶん、イオン、大和ネクスト、ローソン、みんなの、UI、オリックス、GMO あおぞらネット（13 行）。「地域銀行・信金」：地方銀行 62 行、第二地方銀行 37 行、信用金庫 20 金庫（しんきん共同センターに加盟していない信用金庫）。なお、系統中央機関および信託銀行など 16 先は、有効回答が十分に得られなかったことから集計対象外。

[4] アンケート実施期間は、2022 年 4 月 1 日～5 月 31 日まで。回収率は 100%。

２．対顧客チャネル別にみた事務量の増減

調査先における対顧客チャネル別の事務量[5]をみると、店舗窓口や ATM といった対面型チャネルが減少している一方、インターネットバンキングやモバイルアプリといったデジタルチャネルは、モバイルアプリの新規リリース、機能拡張やキャッシュレス決済の拡大等を背景に、大幅に増加している（図表１）。

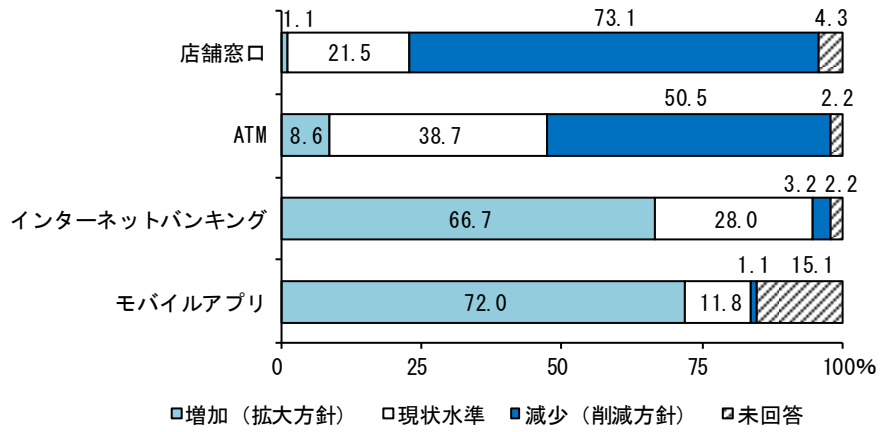
図表１　事務量の推移（月間平均、2018 年度＝100）



（注）集計対象は、2018～2021 年度について回答があった調査先（93 先）。「対面型チャネル」と「デジタルチャネル」では、調査先によって集計方法が異なるため、両者を単純比較できない点には留意が必要。

先行きの事務量の見通しについても、過半の調査先が、対面型チャネルである店舗窓口・ATM の利用減少を見込んでいる一方、デジタルチャネルであるインターネットバンキング・モバイルアプリは更なる利用増加を見込んでおり、対顧客チャネルのデジタル化、非対面化が今後も一段と進展していくとみられる（図表２）。

図表２　チャネル別・事務量の見通し



（注）集計対象は、図表１と同様。

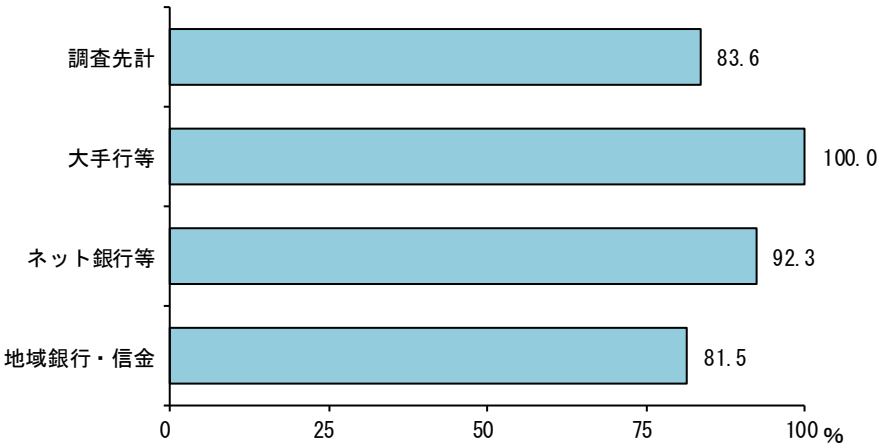
[5] 事務量は「振込、振替、入出金、貸出、残高照会、役務取引等」の件数（調査先の内部管理ベース）をいう。

３．モバイルアプリの提供状況

（１）モバイルアプリの提供拡大

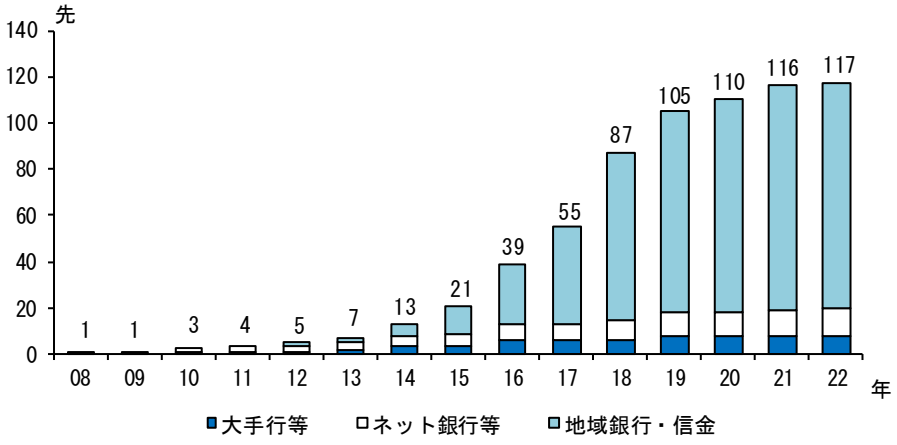
調査先におけるモバイルアプリの提供状況をみると、アンケート回答基準時点（2022 年 3 月末）で 8 割超の先で提供されている（図表 3）。また、モバイルアプリの提供開始時期をみると、2008 年以降、大手行等やネット銀行等が先行する形で提供が始まり、その後、2010 年代半ばからは、地域銀行・信金の提供が増加している（図表 4）。

図表 3　モバイルアプリを提供している調査先の割合



（注）集計対象は、各金融機関が独自に提供しているモバイルアプリに限る。

図表 4　調査先におけるモバイルアプリの提供開始時期



（注）アンケート回答基準時点（2022 年 3 月末）に、モバイル端末向けのアプリ配信プラットフォームに掲載されているモバイルアプリの提供開始時期を集計。

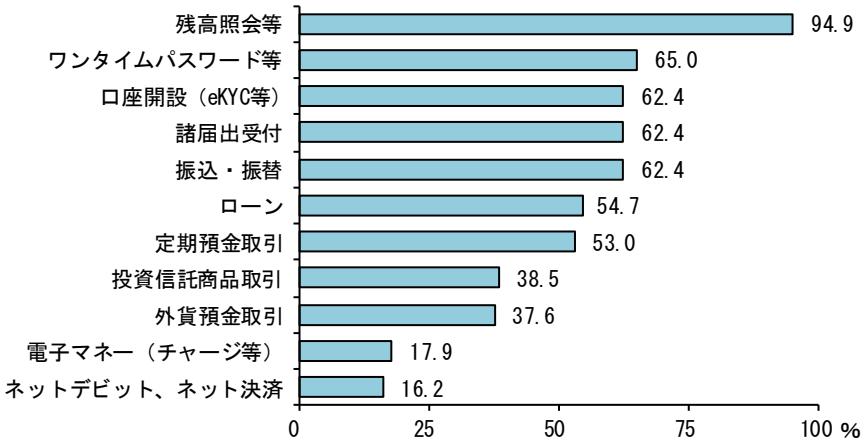
（２）提供サービス

モバイルアプリを提供している調査先における提供サービスの内容をみると、店舗窓口やATM を利用することなく、モバイル端末で金融取引や口座開設が完結できるようセキュリティ機能が実装され、幅広いサービスが提供されている（図表５）。

「残高照会等」は９割超の先で提供済みのほか、「ワンタイムパスワード等」や eKYC[6]等による「口座開設」、名義・住所変更等の「諸届出受付」などの口座管理に係るサービスを提供している先は６割強に達している。また、「振込・振替」や「ローン」、「定期預金取引」も５～6 割の先が提供している。

―― 複数のサービスを提供している調査先をみると、現状では①サービスごとに異なるモバイルアプリを提供するケースと、②１つのモバイルアプリで複数のサービスを提供するケースに分けられる。今後、モバイルアプリの機能拡張に伴い、提供モバイルアプリの一元化が進む可能性もある。

図表５　モバイルアプリによるサービスの提供状況



（注）集計対象は、モバイルアプリを提供している調査先。

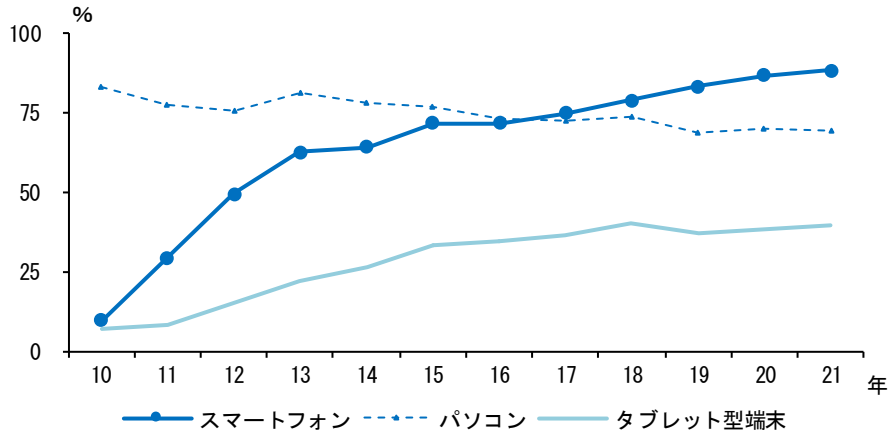
[6] 「eKYC（electronic Know Your Customer）」とは、インターネットを利用してオンラインで本人確認を完結できる仕組みをいう。

BOX インターネットバンキングとモバイルアプリ

スマートフォンの保有率の推移

金融機関では、1990 年代後半以降、インターネットを通じたオンラインでの金融取引サービスである「インターネットバンキング」の提供を始め、これまでの 20 年超の間に、サービス拡充、セキュリティ対策の強化等の様々な施策を実施してきた。こうしたなか、2008 年以降、「モバイルアプリ」の提供が開始され、提供先や機能が拡大していった背景としては、スマートフォンの保有率の上昇（図表 B-1）があげられる。

図表 B-1　主な情報通信機器の世帯保有状況



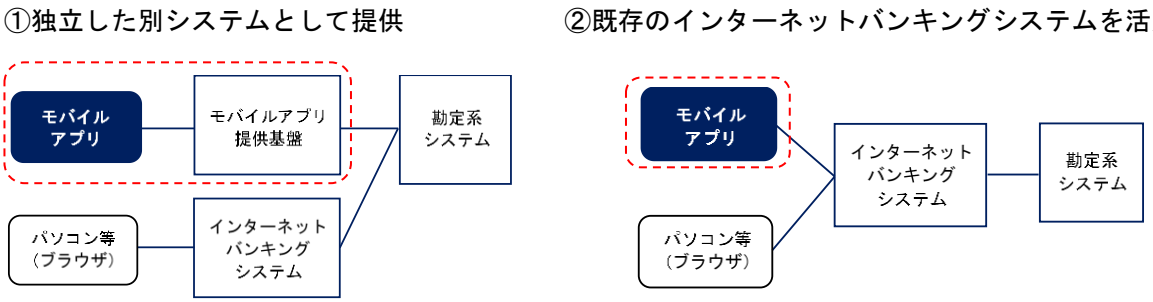
（資料）総務省「通信利用動向調査」

システム構成の比較

技術的な観点から、モバイルアプリのシステム構成をみると、①モバイルアプリとともに、インターネットバンキングシステムとは独立した別システムとして新たにサービス基盤を構築する方式と、②既存のインターネットバンキングシステムを基盤に、新たな対顧客接点としてモバイルアプリを提供する方式の 2 種類がみられた（図表 B-2）。

―― この点、一部の小規模金融機関では、個人向けインターネットバンキングの利用率が伸び悩む中で、共同インターネットバンキングの使用料の負担が重くなっており、モバイルアプリをインターネットバンキングシステムとは独立したサービス基盤により提供することで、将来的にインターネットバンキングの廃止を検討する動きがみられはじめている。

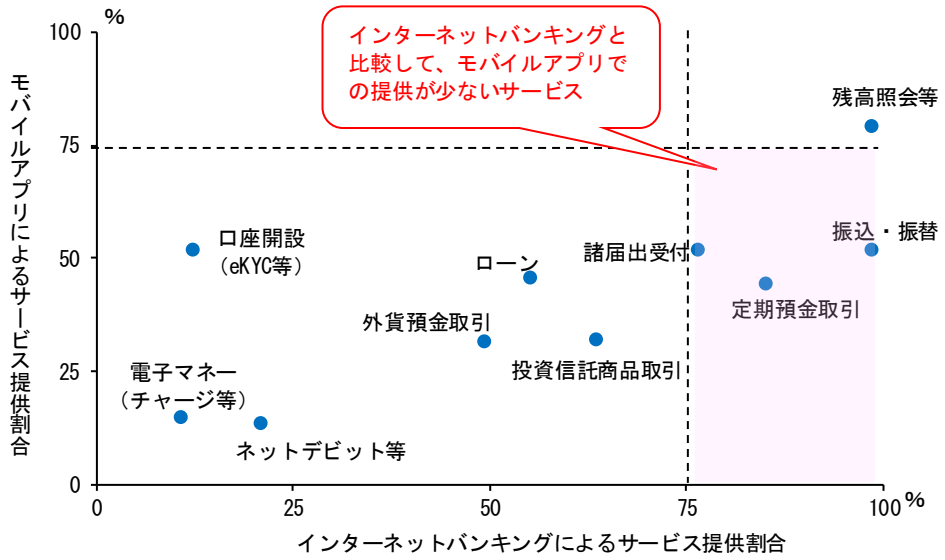
図表 B-2　システム構成のイメージ図



提供サービスの比較

調査先のモバイルアプリとインターネットバンキングのサービス提供状況を比較すると、「振込・振替」や「定期預金取引」、「諸届出受付」は、モバイルアプリでの提供が少ないことが確認された（図表 B-3）。特に「振込・振替」は、インターネットバンキングでは、ほぼすべての先で提供されていた一方、モバイルアプリでの提供先は半数程度の先にとどまっている。今後、モバイルアプリへの顧客ニーズが高まっていくとすれば、モバイルアプリでの資金移動を伴うサービスの提供が拡大していく可能性がある。

図表 B-3　インターネットバンキングとモバイルアプリのサービス比較



（注）集計対象は、調査先。このため、集計対象が「モバイルアプリを提供している調査先」である、図表 5「モバイルアプリによるサービスの提供状況」と計数は一致しない。

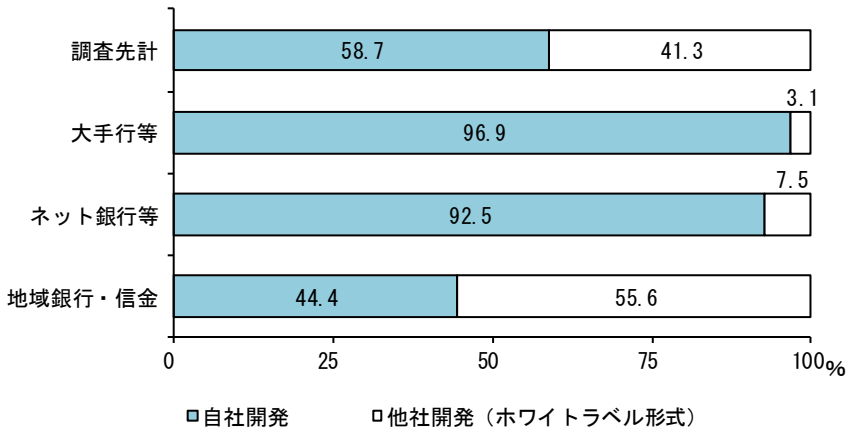
４．モバイルアプリの管理体制

（１）開発形態

モバイルアプリの開発形態は、モバイルアプリを自社で開発するか、他社が開発したモバイルアプリを自社用にカスタマイズするか（ホワイトラベル形式）に大別できる。自社開発では、独自性を発揮し易い一方で、開発期間の長期化や維持・管理負担は大きくなる。アンケート結果をみると、大手行等やネット銀行等のモバイルアプリの多くは自社開発である一方、地域銀行・信金では他社開発（ホワイトラベル形式）を利用しているものが多い[7]（図表6）。

―― ホワイトラベル形式のモバイルアプリの提供元となっている企業をみると、金融機関の勘定系システムの開発・運用を担ってきたシステムベンダーに加えて、FinTech 企業や自社開発のモバイルアプリを他社に販売する金融機関などもみられる。

図表 6　モバイルアプリの開発形態

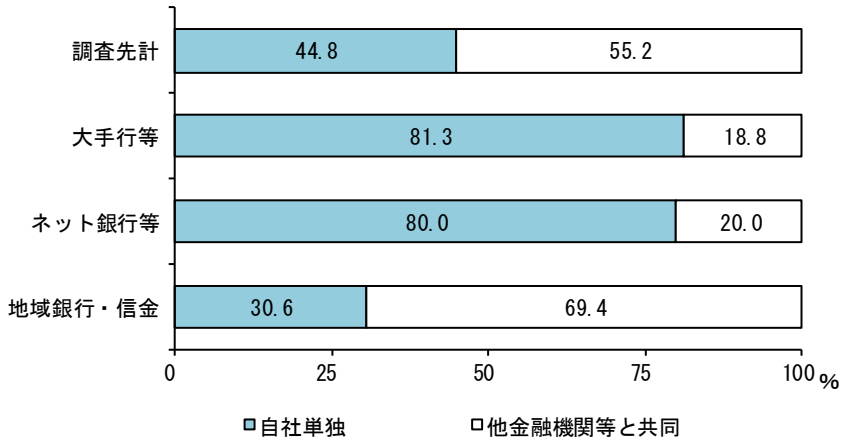


（注）集計対象は、調査先が提供しているモバイルアプリ。

次に、モバイルアプリの提供基盤（サービスを提供するサーバー等）をみると、大手行等やネット銀行等では、自社単独基盤を利用するモバイルアプリが多い一方、地域銀行・信金では、他金融機関等との共同基盤を利用するものが多くみられた（図表７）。リスク管理の観点からは、単独基盤か共同基盤かにかかわらず、システム障害やセキュリティの脆弱性判明時などのインシデントが発生した場合を想定した、適切なリスク評価や委託先管理が必要である。

[7] 他社開発のモバイルアプリ（ホワイトラベル形式）を自社開発のモバイルアプリに組み込んでいる場合、アンケートでは「自社開発」と回答しているケースもある。

図表７　モバイルアプリの提供基盤

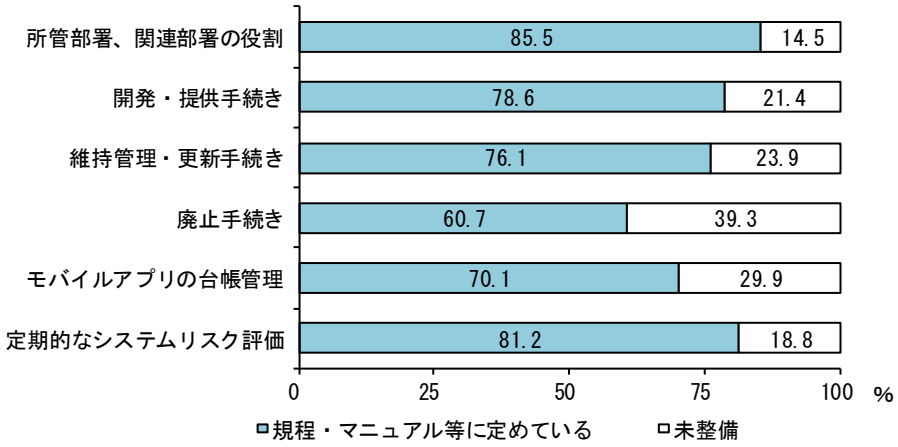


（注）集計対象は、調査先が提供しているモバイルアプリ。

（２）管理体制

モバイルアプリの開発・維持管理・リスク評価に関する管理体制をみると、全体として規程・マニュアル等の整備が進んでいるものの、いずれの項目でも未整備の先が一定数みられた。特にモバイルアプリの台帳管理や廃止手続きを整備していない先が３～４割程度となっている（図表８）。他社開発や共同基盤で利用しているモバイルアプリであっても、自らが提供する対顧客サービスの一翼を担うシステムであることから、通常のシステムと同様にシステムリスク管理の枠組みの対象とするなど、適切な管理体制を整備することが必要である。

図表８　モバイルアプリの管理体制



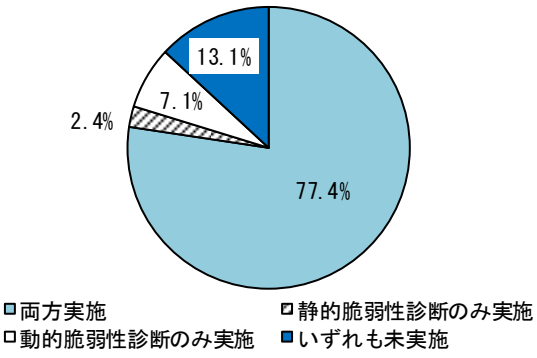
（注）集計対象は、モバイルアプリを提供している調査先。「規程・マニュアル等に定めている」は整備中の先を含む。

（３）脆弱性・セキュリティ対策

モバイルアプリの脆弱性診断の実施状況をみると、多くのモバイルアプリで静的脆弱性診断[8]と動的脆弱性診断[9]の両方、またはいずれかが実施されていたが、いずれの脆弱性診断も実施されていないモバイルアプリが１割程度となっている[10]（図表９）。

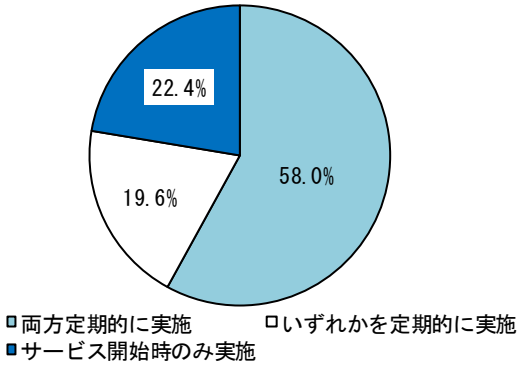
また、脆弱性診断の実施頻度をみると、いずれかの脆弱性診断を定期的に実施しているモバイルアプリが過半数となったものの、サービス開始時のみの実施にとどまっているものも一定数みられた（図表 10）。提供しているサービスの重要度が高い場合には、脆弱性診断を定期的に実施することが適当である。

図表９　モバイルアプリの脆弱性診断の実施状況



（注）集計対象は、調査先が提供しているモバイルアプリ。

図表 10　モバイルアプリの脆弱性診断の実施頻度

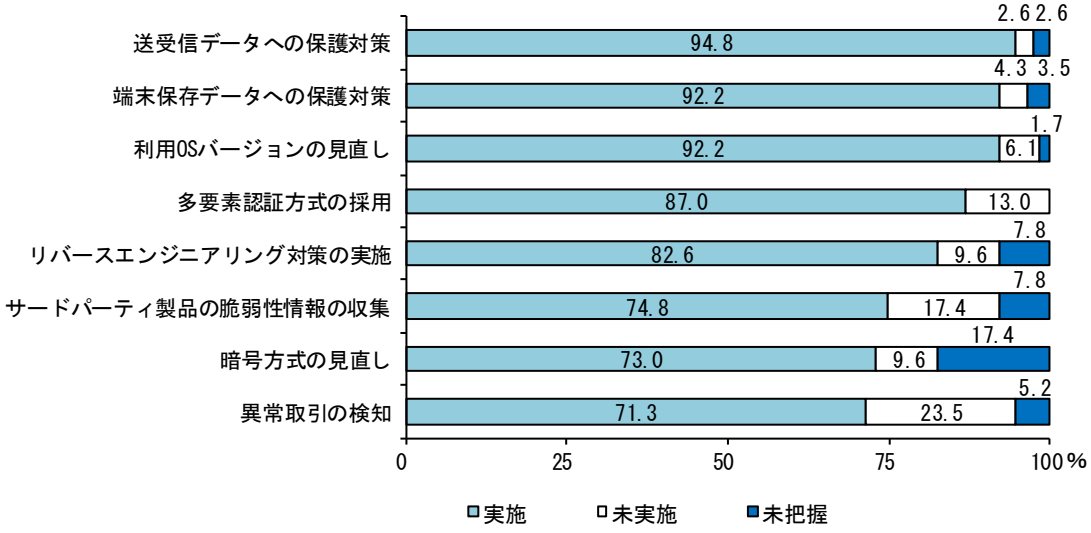


（注）集計対象は、脆弱性診断を実施しているモバイルアプリ。

モバイルアプリのセキュリティ対策の実施状況をみると、データの保護や利用 OS バージョンの見直しなどの対策は、多くの調査先で実施済みとなっているが、サードパーティ製品[11]の脆弱性情報の収集などの対策は「未実施」または「未把握」とする先もみられた（図表 11）。「未把握」と回答した先には、ホワイトラベル形式で他社開発のモバイルアプリを利用している先が少なからず含まれているが、委託先管理の観点からは、セキュリティ対策の実施状況を把握しておく必要がある。

8　「静的脆弱性診断」は、プログラムのコードを分析して、最新の脆弱性情報を用いて検査することをいう。
9　「動的脆弱性診断」は、動作中のモバイルアプリに対して、最新の脆弱性情報を用いて検査することをいう。
10　ただし、脆弱性診断を「いずれも未実施」と回答したモバイルアプリの詳細をみると、ホワイトラベル形式のモバイルアプリやインターネットバンキングへのリンクアプリが多数含まれていることから、別の枠組みのもとで実施済みのものも一定数含まれている可能性がある。
11　「サードパーティ製品」は、モバイルアプリや同提供基盤等に使用される他社の製品をいう。

図表 11　モバイルアプリのセキュリティ対策の実施状況

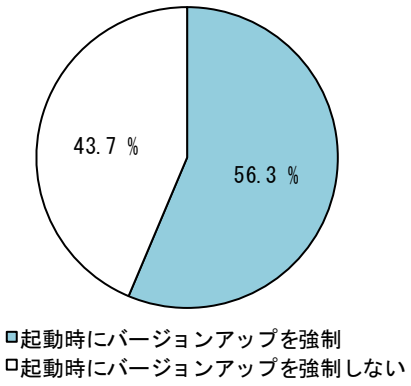


（注）集計対象は、モバイルアプリを提供している調査先。

（4）バージョンアップ時のユーザーへの対応

モバイルアプリにおけるセキュリティ対応を伴うバージョンアップ時の対応をみると、起動時にバージョンアップをユーザーに強制していないものも相応に存在している（図表 12）。この点、提供しているサービスの重要度にもよるが、重大な脆弱性の判明時等、通常のバージョンアップではリスクが解消されない場合には、ユーザーが安全に利用できるようバージョンアップの強制は必要と考えられる。

図表 12　モバイルアプリにおけるセキュリティ対応を伴うバージョンアップ時のユーザーへの対応



（注）集計対象は、調査先が提供しているモバイルアプリ。

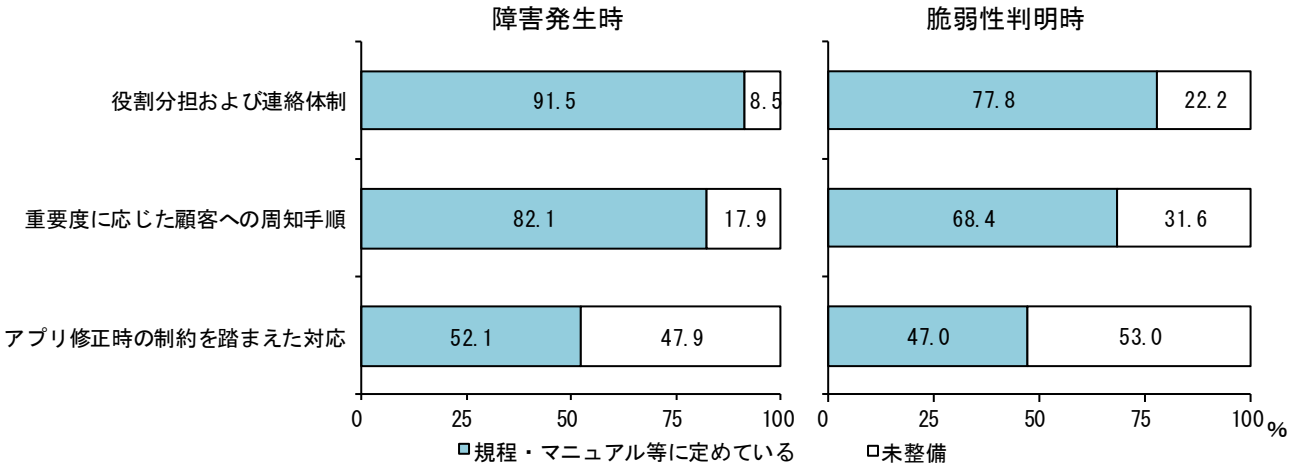
５．インシデント発生時の対応

モバイルアプリにおけるインシデント発生時（システム障害発生時やセキュリティの脆弱性判明時など）の体制や対応手順の整備状況をみると、障害発生時については、「役割分担および連絡体制」、「重要度に応じた顧客への周知手順」が大半の調査先で整備されていたものの、未整備の先も１～２割程度となっている（図表 13）。モバイルアプリの障害発生時には、顧客に対してサービス停止の状況や代替サービス（店舗窓口、ATM 等）の案内等について情報が円滑に伝達されるよう業務継続体制を構築しておくことが重要である。

また、セキュリティの脆弱性判明時は、障害発生時と比べて「役割分担および連絡体制」や「重要度に応じた顧客への周知手順」が未整備の先が多い。今後、モバイルアプリの利用が増加し、機能が拡張されていくことに伴い、重要度の高いサービスが提供される方向にあると考えられる。こうした点も踏まえ、脆弱性のリスクの見極め、対応の必要性を判断する際の考え方や基準、対応手順を事前に検討・整理しておくことは重要である。

なお、モバイルアプリを修正・アップデートする場合には、金融機関またはベンダー等で修正版を作成後、モバイル端末向けのアプリ配信プラットフォームでの所要の審査を経て、同プラットフォームに掲載されるといったプロセスを踏む必要がある。こうした実務的な制約を踏まえた対応に関しては、障害発生時、脆弱性判明時ともに、約半数の先が未整備となっている。手順の整備に当たっては、こうした制約も念頭に置く必要がある。

図表 13　モバイルアプリにおけるインシデント発生時の対応手順の整備状況

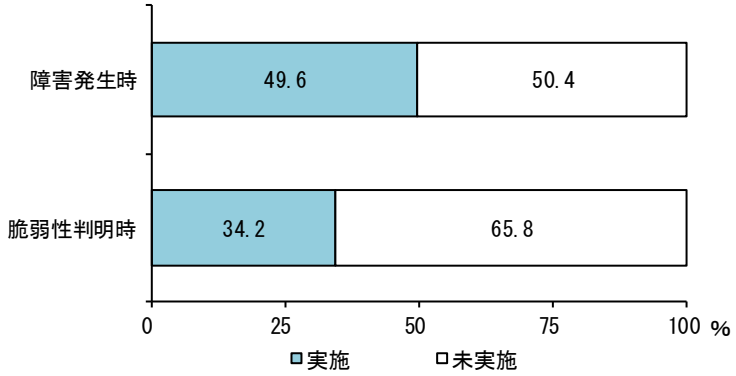


（注 1）集計対象は、モバイルアプリを提供している調査先。「規程・マニュアル等に定めている」は整備中の先を含む。

（注 2）「アプリ修正時の制約を踏まえた対応」とは、モバイルアプリを修正・アップデートする場合、アプリ配信プラットフォームでの所要の審査を経てリリースする必要があり、こうした実務的な制約を踏まえた顧客対応や行内対応手順の整備をいう。

次に、モバイルアプリのインシデント発生時を想定した訓練の実施状況をみると、障害発生時、脆弱性判明時ともに過半数の先が訓練を実施していない（図表 14）。システム障害訓練等のシナリオにモバイルアプリでのインシデント発生時の対応手順を盛り込み、訓練（机上を含む）によりその手順の実効性を向上させることや対応要員の習熟を行うことは重要である。この点、チャネルごとの事務量の動向といった環境変化を踏まえた訓練を定期的に実施することを通じて、想定している業務継続体制の実効性を検証するとともに、管理体制の更なる強化に繋げていくことが期待される。

図表 14　モバイルアプリにおけるインシデント発生時を想定した訓練の実施状況



（注）集計対象は、モバイルアプリを提供している調査先。

6．おわりに

新型コロナウイルス感染症の拡大を受けた非対面型のサービスに対するニーズの高まりもあって、金融機関の対顧客チャネルのうち、デジタルチャネルを通じた事務取扱量が増加している。モバイルアプリは、今後も利便性に優れたデジタルチャネルの中核として更なる利用増加が見込まれている。

金融機関によって、モバイルアプリの開発・管理の形態は異なっているが、自らが提供する対顧客サービスの一翼を担うシステムである以上、これを適切に管理することが求められる。モバイルアプリは、脆弱性対応等のセキュリティ対策が随時必要となることから、影響調査や対策が円滑に実施できるよう、関係先を含めた管理体制の構築が必要である。

金融機関の対顧客チャネルにおけるデジタル化の進展は、顧客の利便性向上に資する一方、インシデントが発生した場合の顧客への影響度は大きくなる。モバイルアプリにおけるインシデント発生時を想定し、顧客に対してサービス停止の状況や代替サービス（店舗窓口、ATM 等）の案内といった情報が円滑に伝達されるよう業務継続体制を構築しておくことが重要である。チャネルごとの事務量の動向といった環境変化を踏まえた訓練（机上を含む）を定期的に実施することを通じて、想定している業務継続体制の実効性を検証するとともに、管理体制の更なる強化に繋げていくことが期待される。

日本銀行としても、今後も考査・モニタリングやセミナーなどを通じて、金融機関のこうした取り組みを後押ししていく方針である。